DII COE 4.1 NT Kernel Security

Lara M. Sosnosky

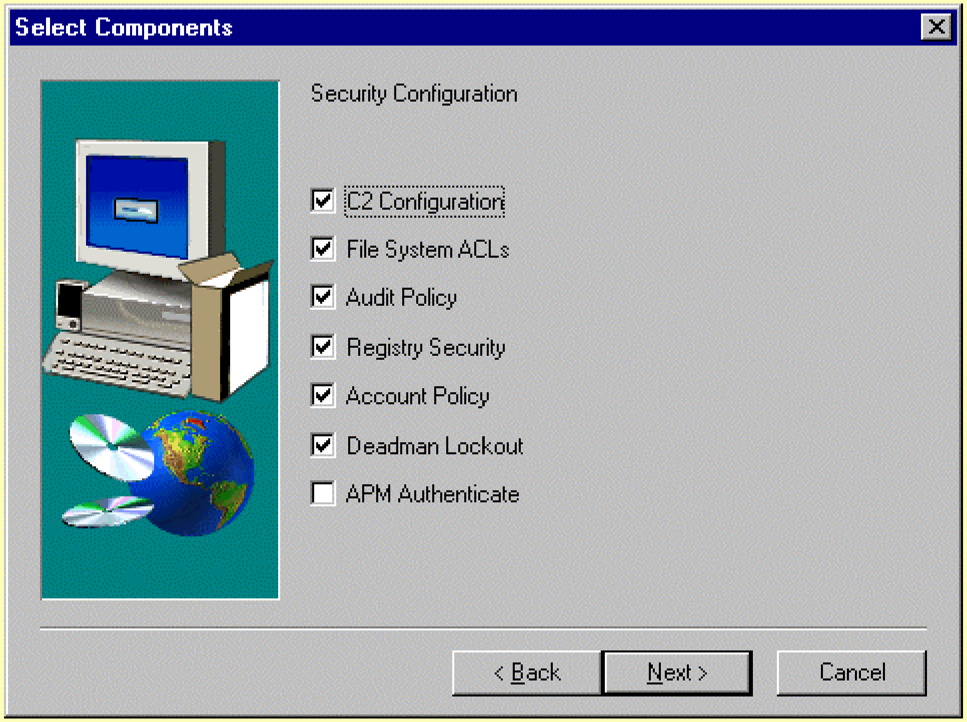
July 8, 1999

COE 4.1 NT Kernel Security

- **Goal: Ship kernel with default security settings**
- **Met with JPL developers in May**
  - **Applied security settings from *Secure Windows NT Installation and Configuration Guide* (based on SRS reqs) and NTSCON scripts**
  - **Provided a “minimum” set of security settings**
  - **Implemented settings through InstallShield during kernel installation**

COE 4.1 NT Kernel Security Settings

- C2 configuration
- Audit policy
- Registry security settings
- Account policy
  - Covers password length, complexity
  - No account lockout policy
- Screensaver policy
  - Password-protected
  - No deadman lockout
- File system and registry ACLs
  - NOT as strict as defined in the I&C guide



Select Components

Security Configuration

☑ C2 Configuration
☑ File System ACLs
☑ Audit Policy
☑ Registry Security
☑ Account Policy
☑ Deadman Lockout
☐ APM Authenticate

COE 4.1 NT Kernel Security

- Configured kernel on Service Pack 4 baseline
- Reviewing APM architecture/security with JPL and DISA
  - Common policy across all 3 platforms
- 4.1 kernel currently runs on NT 4.0 workstation only!
  - Future: 4.1 NT server kernel
- SAIC creating a 4.1 OS patch segment containing:
  - Service Pack 4 (SP4)
  - Post-SP4 hotfixes
  - Y2K fixes
  - Post-SP5 LSA3 hotfix

COE 4.1 Security Configuration Manager Segment

- Plan to create 3 separate segments:
  - First: Full segment containing COTS binaries (SCM, MMC, IE 5)
    - SCM requires MMC and IE 3.02+
    - Using IE 5 since IE 4.01 breaks 4.1 kernel
  - Second: Partial segment to remove IE icon from desktop
    - IE not supported by DISA
  - Third: Data segment containing SCM templates
    - Provide “lock” and “unlock” capability

COE 4.1 Installation

- Order of installation:
  - NT 4.0 operating system
  - SP4
  - 4.1 NT kernel
  - OS patch
  - SCM segments

- NOTE: Current 4.1 kernel will not install on a machine with SP5 preloaded